STATE OF ALABAMA

Information Technology Standard

STANDARD 662S1-00: SERVER SECURITY

Though operating system vendors have taken steps to make their operating system baseline configurations more secure on a default installation, additional operating system hardening efforts are usually required to enhance the confidentiality, integrity, and availability of the data present on the servers and accountability in regards to persons authorized access to the servers as well as complete restriction of unauthorized access. Furthermore, dependent on server functionality (e.g., domain controllers or Web servers) additional hardening must be considered based on the server's level of exposure to cyber threats. In order to reduce the exposure of State of Alabama server-based computing resources to cyber-related threats and unauthorized access, secure operating system baseline configurations are necessary as a fundamental countermeasure.

OBJECTIVE:

Define standard configuration settings for a secure operating system computing baseline for State of Alabama server computing resources.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

The following requirements, based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-123: Guide to General Server Security, apply to State of Alabama servers. System-specific security settings apply to servers utilizing Microsoft Windows Server 2003 and Windows Server 2008.

GENERAL SERVER SECURITY

Physical Security:

- Place servers in secured areas with controlled access.
- Additional physical security requirements are stated in State IT Policy 651: Physical Security.

Server Hardening:

Install only the services required for the server and eliminate any known vulnerabilities through patches or upgrades. Any unnecessary applications, services, or scripts that are installed should be removed immediately once the installation process is complete.

During the installation of the server software, the following steps should be performed:

- Install the server software either on a dedicated host or on a dedicated guest operating system (OS) if virtualization is being employed.
- Apply any patches or upgrades to correct for known vulnerabilities in the server software.
- Create a dedicated physical disk or logical partition (separate from OS and server application) for server data, if applicable.
- Remove or disable all services installed by the server application but not required (e.g., gopher, FTP, HTTP, remote administration).
- Remove or disable all unneeded default user accounts created by the server installation.

- Remove all manufacturers' documentation from the server.
- Remove all example or test files from the server, including sample content, scripts, and executable code.
- Remove all unneeded compilers.
- Apply the appropriate security template or hardening script to the server.
- Configure each network service to listen for client connections on only the necessary TCP and UDP ports, if possible.

Consider installing the server with non-standard directory names, directory locations, and filenames if possible. Many server attack tools and worms targeting servers only look for files and directories in their default locations. While this will not stop determined attackers, it will force them to work harder to compromise the server, and it also increases the likelihood of attack detection because of the failed attempts to access the default filenames and directories and the additional time needed to perform an attack.

SYSTEM-SPECIFIC SECURITY SETTINGS

To determine the specific security settings to use, organizations first need to determine the server's role (domain controller, file server, Web server, etc.) and the appropriate operating environment (Legacy Client, Enterprise Client, or Specialized Security – Limited Functionality (SSLF)) based on the client types supported and/or the need for tighter security.

Document the designated operating environment and server role in system security plans and local operating procedures.

Windows Server 2003:

The Microsoft publication, Windows Server 2003 Security Guide, provides the baseline configuration to be implemented on all State of Alabama servers running the Windows Server 2003 operating system.

Download the Windows Server 2003 Security Guide from the Microsoft Download Center: http://www.microsoft.com/downloads/details.aspx?familyid=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en

Windows Server 2008:

The Microsoft publication, Windows Server 2008 Security Guide, provides the baseline configuration to be implemented on all State of Alabama servers running the Windows Server 2008 operating system.

Download the Windows Server 2008 Security Guide from the Microsoft Download Center: http://www.microsoft.com/downloads/details.aspx?FamilyID=fb8b981f-227c-4af6-a44b-b115696a80ac&DisplayLang=en

MAINTAINING SERVER SECURITY

Securely administering a server on a daily basis is an essential aspect of server security. Maintaining the security of a server requires:

- Backing up critical information
- Configuring, protecting, and analyzing log files
- Establishing procedures for recovering from server compromise
- Routinely and proactively updating systems with fixes, patches, definitions, and service packs
- Testing security periodically

ADDITIONAL INFORMATION:

Information Technology Policy 662: Systems Security
http://cybersecurity.alabama.gov/documents/Policy_662_Systems_Security.pdf

Information Technology Policy 651: Physical Security
http://cybersecurity.alabama.gov/documents/Policy_651_Physical_Security.pdf

Information Technology Standard 662S2: Client Systems Security
http://cybersecurity.alabama.gov/documents/Standard_662S2_Client_Systems_Security.pdf

Information Technology Standard 662S3: Point-of-Sale Systems Security
http://cybersecurity.alabama.gov/documents/Standard_662S3_POS_Systems_Security.pdf

Information Technology Guideline 662G1: Systems Security
http://cybersecurity.alabama.gov/documents/Guideline_662G1_Systems_Security.pdf

Information Technology Dictionary
http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
660-02B1	12/18/2007	Original Baseline document
660-02B1_A	9/18/2008	Added general security requirements from NIST 800-123 and Windows Server 2008 Security Guide reference.
660-02S3	2/4/2011	Reissued as a Standard
662S1-00	09/01/2011	New number and format